SI 2.2.1

- **La confidencialidad.** Solo pueden acceder a la información aquellas personas autorizadas.
- **Disponibilidad.** La información siempre está disponible para aquellos que la necesiten.
- **Autorización.** Una vez identificados los usuarios, estos pueden tener privilegios.
- **Accounting.** Se realiza un seguimiento de las acciones que realiza un usuario.
- **Vulnerabilidad.** Un sistema puede ser atacado mediante un efecto y puede ser reconocido o no.
- **Impacto.** Daño producido en un ataque.
- **Plan de contingencia.** Prevención de un sistema para evitar un desastre. Se evalúa el peligro, planificar una recuperación total y evaluar su eficiencia y eficacia.

SI 2.3

1. **En el cuaderno de clase enumera 5 casos en los que alguien quisiera utilizar algún método que violara la seguridad, porque quiere vulnerar la seguridad y con qué fin.**

- Interrupción: hacer caer un servidor de la competencia.
- Interceptación: para conseguir información importante.
- Suplantación: creando emails falsos para atacarte.
- Modificación: modificar el código de un programa con un fin de estafa.
- Suplantación: creando paginas web falsas para obtener datos financieros.

SI - SEGURIDAD FÍSICA Y LÓGICA

2. Piensa en los perfiles de atacantes que hay en el tema. ¿Hay alguien en tu clase que creas que el día de mañana pueda responder a un de ellos? Explica por qué, aunque no pongas el nombre propio.

Sí, lammers. Por lo que están estudiando probablemente más de uno se crea Hacker en un futuro.

3. De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)

    a. Ventilador de un equipo informático. Activa/Física
    b. Detector de incendio. Pasiva/Física
    c. Detector de movimientos. Activa/Física
    d. Cámara de seguridad. Pasiva/Física
    e. Cortafuegos. Activa/Lógica
    f. SAI. Pasiva/Fisica
    g. Control de acceso mediante el iris del ojo. Activa/Física
    h. Contraseña para acceder a un equipo. Activa/Lógica
    i. Control de acceso a un edificio. Activa/Física

4. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.

    a. Terremoto. Física
    b. Subida de tensión. Física
    c. Virus informático. Lógica
    d. Hacker. Lógica
    e. Incendio fortuito. Física
    f. Borrado de información importante. Lógica

5. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.

    a. Antivirus. Activa/Pasiva
    b. Uso de contraseñas. Activa
    c. Copias de seguridad. Pasiva
    d. Climatizadores. Activa
    e. Uso de redundancia en discos. Pasiva
    f. Cámaras de seguridad. Pasiva
    g. Cortafuegos. Activa

6. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:

    a. mesa. No, con un diccionario se rompe fácilmente.
    b. caseta. No, con un diccionario se rompe fácilmente.
    c. c8m4r2nes. Si, la mezcla de números y letras es mucho más seguro.
    d. tu primer apellido. No, muy sencillo de averiguar.
    e. pr0mer1s&. Si, la mezcla de números y letras es mucho más seguro.

f. tu nombre. No, muy sencillo de averiguar.

7. Ordena de mayor a menor seguridad los siguientes formatos de claves.
   a. Claves con sólo números.
   b. Claves con números, letras mayúsculas y letras minúsculas.
   c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.
   d. Claves con números y letras minúsculas.
   e. Claves con sólo letras minúsculas.

   c > b > d > e > a

1. En el cuaderno de clase enumera 5 casos en los que alguien quisiera utilizar algún método que violara la seguridad, porque quiere vulnerar la seguridad y con qué fin.

   - Interrupción: hacer caer un servidor de la competencia.
   - Interceptación: para conseguir información importante.
   - Suplantación: creando emails falsos para atacarte.
   - Modificación: modificar el código de un programa con un fin de estafa.
   - Suplantación: creando paginas web falsas para obtener datos financieros.

2. Busca qué es una ACL, entiéndelo, y explícalo en clase.

   Lista de control de acceso. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

3. Busca qué es sfc, entiéndelo, y explícalo en clase.

   Es un comando que analiza todos los archivos protegidos del sistema y reemplaza los archivos dañados con una copia almacenada en caché.

4. Describe los medios de seguridad física y lógica que hay en el aula.

   Física: extintor, espacio.
   Lógica: contraseñas

5. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.
   Activa: contraseña, antivirus.
   Pasiva: copia de seguridad, antivirus, SAI.

6. Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.

   - Redactar y revisar planes de actuación ante catástrofes.
   - Gestionar y revisar los logs de las aplicaciones y el sistema operativo.
   - Hacer controles de acceso físico al sistema como pueden ser las tarjetas de identificación
   - Control de la temperatura y la humedad de la habitación donde se encuentran los ordenadores.

7. Busca en Internet las claves más comúnmente usadas.

   1.- 123456 (Primer puesto por segundo año consecutivo)
   2.- password (Segundo puesto por segundo año consecutivo)
   3.- 12345678 (Sube un puesto)
   4.- qwerty (Sube un puesto)
   5.- 12345 (Baja dos puestos)
   6.- 123456789 (Se mantiene)
   7.- football (Sube tres puestos)
   8.- 1234 (Baja un puesto)
   9.- 1234567 (Sube dos puestos)
   10.- baseball (Sube dos puestos)
   11.- welcome (Nueva)
   12.- 1234567890 (Nueva)
   13.- abc123 (Sube un puesto)
   14.- 111111 (Sube un puesto)
   15.- 1qaz2wsx (Nueva)
   16.- dragon (Baja siete puestos)
   17.- master (Sube dos puestos)
   18.- monkey (Baja seis puestos)

19.- letmein (Baja seis puestos)
20.- login (Nueva)
21.- princess (Nueva)
22.- qwertyuiop (Nueva)
23.- solo (Nueva)
24.- passw0rd (Nueva)
25.- starwars (Nueva)

8. Decides montar una empresa en Internet que se va a dedicar a ofrecer un disco duro on-line. Necesitas de cada usuario: nombre, teléfono y dirección de correo electrónico. ¿En qué afectar estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información?

   Encriptación de datos, copias de seguridad

9. Busca en Internet un protocolo de actuación ante un desastre natural, cita las cosas que veas interesantes (que tipo de personas interviene), pues las vas a explicar en clase, y añade a ese protocolo las medidas que consideres para no perder la información de la organización.